



# **Cloud Computing at CDC Current Status and Future Plans**

**Earl Baum**

**March, 2014**

# Agenda

- Background
- Current Activities
- Use Cases, Shared Services and Other Considerations
- What's Next



# Background – Cloud Definition

- NIST Special Publication 800-145 identifies five essential characteristics of cloud systems:
  - **On-demand self-service.** The customer can, on their own, provision computing additional computing resources without the need for human interaction with each service provider (e.g. pay only for the resources you need, add more as your demands grow).
  - **Broad network access.** The system and its capabilities are available over the network and accessed through standard mechanisms (e.g., mobile phones, tablets, laptops, and workstations).
  - **Resource pooling.** Computing resources are pooled to serve multiple customers with different physical and virtual resources and can dynamically be assigned and reassigned according to demand. Examples of resources include storage, processing, memory, and network bandwidth.
  - **Rapid elasticity.** Computing resources can be provisioned and released, in some cases automatically, to rapidly grow or shrink based on demand (e.g. configure thresholds to allocate or release processing power, storage, etc.).
  - **Measured service.** Cloud systems can automatically control and optimize resources based on things like storage, processing, bandwidth, and the number of active user accounts. Resource usage can be monitored, controlled, and reported (e.g. ability to see how much bandwidth, storage, processing power, etc. that you are using).



# Background – History

- OMB “Cloud First” Mandate - 2010
- HHS Cloud Reference Architecture – September 2010
- Federal Cloud Computing Strategy – February 2011
- GSA FedRamp – December 2011
- First FedRAMP IaaS ATOs - 2013



# CDC Cloud – Current Activities

- CDC is conducting a Cloud Proof of Concept using Amazon Web Services
- Goal:
  - Identify, develop and implement services and processes required to effectively support CDC systems in a cloud-hosted environment
- Status:
  - Started August 2013, ongoing
  - On track to complete testing and validation of core ITSO services before the end of April, 2014



# CDC Cloud – Procurement

- CDC is developing a dedicated CDC Cloud BPA
  - In-progress – Q3 FY14
- Close coordination of Cloud Procurement within CDC OCIO is required to reduce risks of:
  - Increased costs
    - “Sprawl” – many independent contracts
    - Duplication of services and associated costs
  - Security risks
    - Inconsistent contract language
    - Inconsistent policy interpretation and implementation
    - Larger “surface area” for hackers to attack



So... we have a CDC Cloud...

**NOW WHAT?**



U.S. Department of Health and Human Services  
Centers for Disease Control and Prevention

# Cloud Impact on CDC IT

- Cloud Computing changes the way ITSO provisions some IT services:
  - Core IT services (patching, backup, disaster recovery, authentication)
  - Security-related services (DMZ, monitoring, intrusion detection/prevention)
  - Application/System Development (best practices, SDLC, EPLC)
- Cloud requires consulting services and education
  - Assistance with Analysis of Alternatives, EPLC, Service Architecture, Development Best Practices, Security Integration



# Cloud Impact on C&A

- FedRAMP simplifies the C&A process, but does not eliminate requirements for due diligence and CDC C&A
- Layered components can simplify Cloud C&A:
  - CSP FedRAMP ATO
  - CDC Service/Secure Baseline Configuration (SBC) C&A
  - CDC Application/System C&A



# Shared Service Requirements

- Each Cloud Use Case implies a stack of services (network, security, application interfaces, authentication, firewalls and related items), which must be developed and delivered within the Cloud environment
- These shared services form the framework within which cloud-hosted applications operate
- ITSO, MISO, OCISO and EITPO/EA are working together to develop and provide this service stack



# Cloud Use Cases

- Public-Facing/Public Access, with no access to internal systems
- Public-Facing/Public Access, with access to internal systems
- Public-Facing/Limited Access, requiring login and access to internal systems
- Internally-Facing/Limited Access, requiring login
- Public-Facing Dev-Test/Limited Access, requiring login and access to internal systems
- Internally-Facing Dev-Test/Limited Access, requiring login and access to internal systems
- Batch/On-Demand HPC/Limited Access, requiring login and access to internal systems
- Batch/On-Demand Big Data (Hadoop or similar)/ Limited Access, requiring login and access to internal systems



# What's Next?

- Based on the results of the Amazon Proof Of Concept
  - Finalize and issue the CDC BPA
  - Implement service architecture and processes developed during the POC
- Continue development of Cloud Services and Standards
  - ITSO Cloud WG
  - OCIO Cloud Services Architecture Workgroup
  - Integration with Shared Services Workgroup
- Update EPLC and Analysis of Alternatives to reflect new services and associated best practices
- Education
  - Role-based training for architects, developers and operations staff



# Additional References and Resources

- GSA FedRamp Compliant CSP List
  - <http://www.gsa.gov/portal/content/131931>
- AWS Overview
  - [http://media.amazonwebservices.com/AWS\\_Overview.pdf](http://media.amazonwebservices.com/AWS_Overview.pdf)
- Amazon free training
  - [http://aws.amazon.com/training/intro\\_series/](http://aws.amazon.com/training/intro_series/)
- Application Migration and AWS
  - <http://media.amazonwebservices.com/CloudMigration-main.pdf>



# Architectural Best Practices

- To realize the benefits of the cloud...
  - Design for failure
  - Loose Coupling
  - Elasticity
  - Security
  - Parallel processing for scalability
  - Storage
  - Governance



# Design for Failure

- Avoid single points of failure
  - Infrastructure
  - Services
  - Application Modules
- Assume that everything fails
  - Applications should continue to function even when underlying hardware fails or is removed/replaced



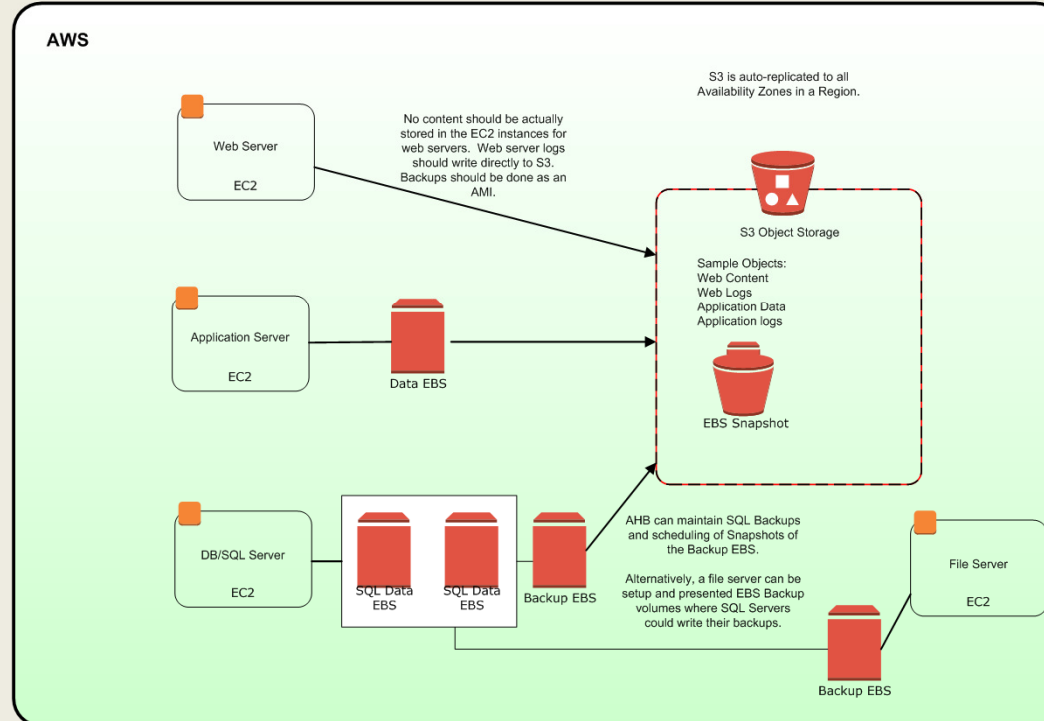
# Backup/Recovery/Resiliency



## AHB

Data Flow Design Diagram  
Cloud Storage/Backup  
Strategy

Draft Ver: 1.0 Date: 2/05/14



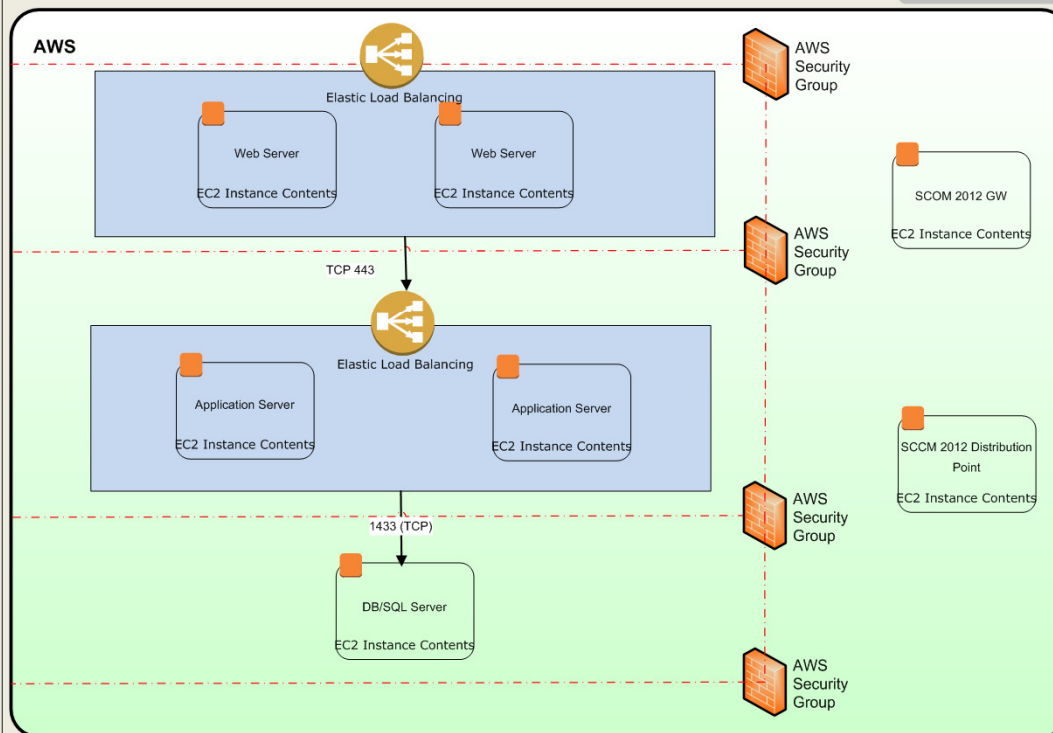
# Monitor/Patch



## AHB

Data Flow Design Diagram  
Cloud Monitoring and Patching

Draft Ver: 1.0      Date: 2/05/14



# Loose Coupling

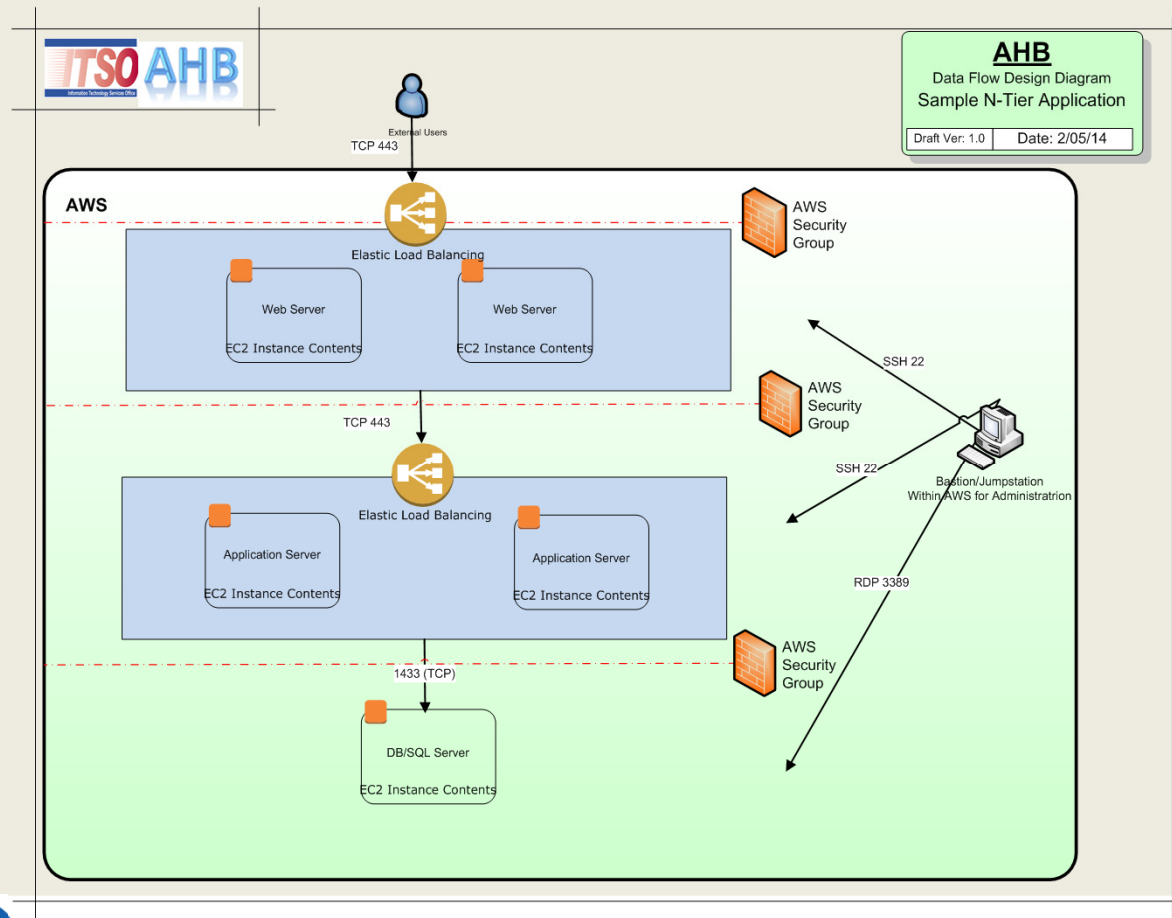
- Design around independent components
  - The more loosely they're coupled, the bigger they scale
- Design app and service components as “black boxes”
  - Input, process, output – without knowledge of the source of inputs or destination of outputs
  - Message queues to link modules
  - Load balancers for clusters



# Elasticity

- The cloud is flexible – or can be...
  - Don't assume the health, availability or fixed location (IP address or server name, for example) of individual components
  - Design application modules so they continue to function through server reboot/relaunch
  - Use dynamic configurations – servers download specifics during bootstrap rather than using fixed internal configs

# Notional Application Architecture



# Security

- Security is still a concern
  - Encrypt data at rest and in transit
  - Use least-privilege model
  - Use granular access-control lists for each function
    - APIs
    - Ports
    - Users
  - Authentication



# Parallel Processing

- Modular code can scale more simply than serial code
- Scale horizontally, rather than vertically
  - Add instances when needed, discard when no longer necessary
  - Depends on service architecture to implement

# Storage

- Multiple options – one size does not fit all
  - Object storage (AWS Elastic Block Store)
    - NAS-equivalent
    - Can be mapped as drives/shares to running instances
  - Block storage (Amazon S3)
    - Write once, read many (NetFlix uses this to store movie images, for example)
  - Archival Storage (Amazon Glacier)
    - Long-Term, low cost, low performance, high availability

# Governance

## Why?

- Consistent, cloud centered decision-making processes, policies, planning, architecture, acquisition, deployment, operation and management
- End-to-end lifecycle management
- Balance cloud investment opportunities and risks
- Avoidance of cloud “sprawl” and unauthorized cloud procurement/deployment



# Governance

## How?

- CDC EPLC:
  - Initiation point for Cloud Governance at the project level, via Stage Gate reviews and the Analysis of Alternatives
- Procurement Reviews
  - Identifying Cloud activities that may fall outside of EPLC
- ITSO Internal Processes
  - Integrate Cloud into existing processes
  - Establish consistent business processes and workflows for Cloud deployments
- OCISO C&A Process
  - Cloud-hosted services still require full C&A

